FortiManager - Managing FortiOS and FSSO

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

November 2, 2017
FortiManager Managing FortiOS and FSSO
02-000-450039-20171102

TABLE OF CONTENTS

Change Log **4**

Introduction **5**

FSSO 5

Agents used in FSSO implementation 6

Domain Controller agent 6

eDirectory agent 6

Citrix/Terminal Server (TS) agent 6

Collector agent 6

DC agent mode and polling mode 7

FortiOS and FSSO **8**

Summary of FortiOS and FSSO scenarios 8

FortiOS with built-in FSSO polling 8

FortiOS with external FSSO polling 9

FortiOS and FortiAuthenticator 9

FortiOS and FSSO CA 10

FortiManager, FortiOS, and FSSO **12**

FortiManager configured with access to FSSO CA 12

FortiAuthenticator support (CA server access) 13

FortiManager configured without access to FSSO CA 14

FortiAuthenticator support (CA server inaccessible) 15

Change Log

Date	Change Description
2017-11-02	Initial release.

Introduction

This document provides summary information on FSSO and the components used for FSSO. It also describes several scenarios involving FortiOS, FSSO, and FortiAuthenticator, and then it describes how FortiManager can be used with FortiOS, FSSO, and FortiAuthenticator.

The purpose of this document is to describe how FortiManager can be used with FortiOS and FSSO, including FortiAuthenticator. This document is not intended to describe the best FSSO solution. The best Fortinet FSSO solution is to use FortiOS Security Fabric with FortiAuthenticator and FortiClient FSSO Mobility agent for the highest polling accuracy. For more information, see the FortiAuthenticator documentation on the Document Library at http://docs.fortinet.com/.

FSSO

This section provides a summary of how FSSO works with FortiGate and FortiManager. FSSO, through agents installed on the network, monitors user logons and passes that information to the FortiGate unit. FSSO can also pass the information to FortiManager, which then passes it to a managed FortiGate. When a user logs on at a workstation in a monitored domain, FSSO:

1. Detects the logon event and records the workstation name, domain, and user
2. Resolves the workstation name to an IP address
3. Determines which user groups the user belongs to
4. Sends the user logon information, including IP address and groups list, and AD group information to the FortiGate or FortiManager unit
5. Creates one or more log entries on the FortiGate or FortiManager unit for this logon event as appropriate

When the user tries to access network resources, the FortiGate unit selects the appropriate security policy for the destination. If the user belongs to one of the permitted user groups associated with that policy, the connection is allowed. Otherwise the connection is denied. With user information such as IP address and user group memberships from the network, you can allow authenticated network access to users who belong to the appropriate user groups without requesting their credentials again. The benefit is users can log in once when connecting to the internal network behind the FortiGate and be automatically logged into servers and services that support Single Sign-On (SSO).

The following types of data are sent from FSSO to FortiGate/FortiManager:

- **AD group information:** configuration data provided by Collector to FortiGate or FortiManager. FortiGate or FortiManager use the data to build local configuration.
- **Logon/logoff event information:** dynamic, real-time information the FortiGate learns and uses to dynamically match against policies and set up connections internally so the user is known without prompting them to log on again.

For more information on FSSO, see the FortiOS documentation at docs.fortinet.com.

Agents used in FSSO implementation

This document refers to different FSSO agents that can be used in an FSSO implementation:

- Domain Controller (DC) agent
- eDirectory agent
- Citrix/Terminal Server (TS) agent
- Collector agent (CA)

Use this section to get familiar with the different agents referenced in this document.

Domain Controller agent

The DC agent must be installed on every domain controller if you will use DC agent mode, but is not required if you use polling mode. See DC agent mode and polling mode on page 7.

eDirectory agent

The eDirectory agent is installed on a Novell network to monitor user logons and send the required information to the FortiGate unit. It functions much like the Collector agent on a Windows AD domain controller.The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.

Citrix/Terminal Server (TS) agent

The Citrix/Terminal Server (TS) agent is installed on a Citrix terminal server to monitor user logons in real time. It functions much like the DC Agent on a Windows AD domain controller.

Collector agent

The CA is installed as a service on a server in the Windows AD network to collect and compile information about user logons, and then send the required information to the FortiGate unit or FortiManager unit, according to Group Filter settings. The CA can collect information from the following agents:

- DC agent (Windows AD)
- TS agent (Citrix Terminal Server)

In a Windows AD network, the CA can optionally obtain logon information by polling the AD domain controllers. In this case, DC agents are not needed.

The CA is responsible for DNS lookups, group verification, workstation checks, and as mentioned FortiGate updates of logon records. The FSSO CA sends AD group membership information to FortiGate units. The CA communicates with the FortiGate over TCP port 8000, and the CA and TS agents also listen on UDP port 8002 for updates from the DC agents.

When using the GUI, you can configure the FortiGate unit to have up to five CAs for redundancy. If the first on the list is unreachable, the next is attempted, and so on down the list until one is contacted. FortiGate does not fallback to a CA agent when a previously unreachable agents returns online again. FortiGate uses only one CA at a time.

All DC agents must point to the correct CA port number and IP address on domains with multiple DCs. If you want to achieve redundancy with two or more Collectors inside the same network, all the DC/TS agents must report to all CA agents.

DC agent mode and polling mode

This section describes the DC agent mode and polling mode referenced in this document.

DC agent mode is sometimes called agent mode, and polling mode is sometimes called agent-less mode.

FSSO for Windows AD requires at least one CA. DC agents may also be required depending on the CA working mode. There are two working modes to monitor user logon activity: DC agent mode or polling mode.

	DC agent mode	Polling mode
Installation	Complex — multiple installations: one agent per DC plus CA, requires a reboot	Easy — only CA installation, no reboot required
Resources	Shares resources with DC system	Has own resources However, if polling is done from CA installed on DC, then DC resources are used.
Network load	Each DC agent requires minimum 64kpbs bandwidth, adding to network load	Advanced users might increase polling period during busy period to reduce network load
Confidence level	Captures all logons	For NetAPI mode, potential to miss a login if polling period is too great

DC agent mode is the standard mode for FSSO. In DC agent mode, a Fortinet authentication agent is installed on each domain controller. These DC agents monitor user logon events and pass the information to the CA, which stores the information and sends it to the FortiGate unit. DC agent mode provides reliable user logon information, however you must install a DC agent on every domain controller. A reboot is needed after the agent is installed. Each installation requires some maintenance as well. For these reasons it may not be possible to use DC agent mode.

In polling mode, the CA polls port 445 of each DC for user logon information every few seconds and forwards it to the FortiGate unit. A major benefit of polling mode is that no FSSO DC agents are required. If it is not possible to install FSSO DC agents on your domain controllers, this is the alternate configuration available to you. Polling mode results in a less complex install. The minimum permissions required in polling mode are to read the event log or call NetAPI.

Note that you should always configure more than one CA. If using DC agents, ensure all DC agents are aware of all CAs.

You should also add service accounts to the Ignore User List in the CA to avoid having service account logins overwrite end user logins on the same workstation.

FortiOS and FSSO

This section describes several scenarios about using FortiOS and FSSO.

This section describes several FortiOS and FSSO scenarios that exclude FortiManager to provide background information before reading the section in this document that describes the same scenarios, but with FortiManager. This document does not strive to recommend one FSSO scenario over another.

Summary of FortiOS and FSSO scenarios

Following is a summary of the scenarios described in this section:

Scenario	Advantage	Disadvantage
FortiOS with built-in FSSO polling	• Simple configuration • No need to install FSSO CA on third party host	• Limited number of monitored DCs • No user logout monitor
FortiOS and FortiAuthenticator	• FSSO CA machine uses own resources • Supports TS, syslog sources, RADIUS accounting, multiple domain environments, FortiClient mobile	• NTLM is supported, but only for one domain. • Citrix support requires TS agent to be installed
FortiOS and FSSO CA	• FSSO CA machine uses own resources • Supports TS, Citrix, RADIUS accounting, NTLM, multiple domain environments	Possible delayed logoff detection

Some FSSO methods are less accurate than others, which is an inherent limitation of the method used to authenticate users. It's unrelated to how Fortinet implemented any of the methods.

FortiOS with built-in FSSO polling

FortiOS with a built-in FSSO CA is suited for a small AD environment. In this scenario, the FortiGate acts as the FSSO CA and queries AD domain controllers for login events. The number of supported domain controllers depends on the

FortiGate model used.

The advantage of this scenario is that configuration is simple, since there is no need to install an FSSO CA on a third party host. The downside of this scenario is that there is a limited number of monitored DCs and no user logout monitor.

This scenario is ideal for a small AD environment, where the monitored DCs are physically close to the FortiGate and latency is low. This scenario is not ideal for a large environment where the FortiGate needs to spend significant resources to query a large list of DCs and/or poll a large LDAP tree.

In a scenario with multiple sites, where each FortiGate only monitors events from local server(s), each polling server must be configured with an ID unique across all sites. When FortiManager retrieves the configuration from each FortiGate, the ID should not be overwritten.

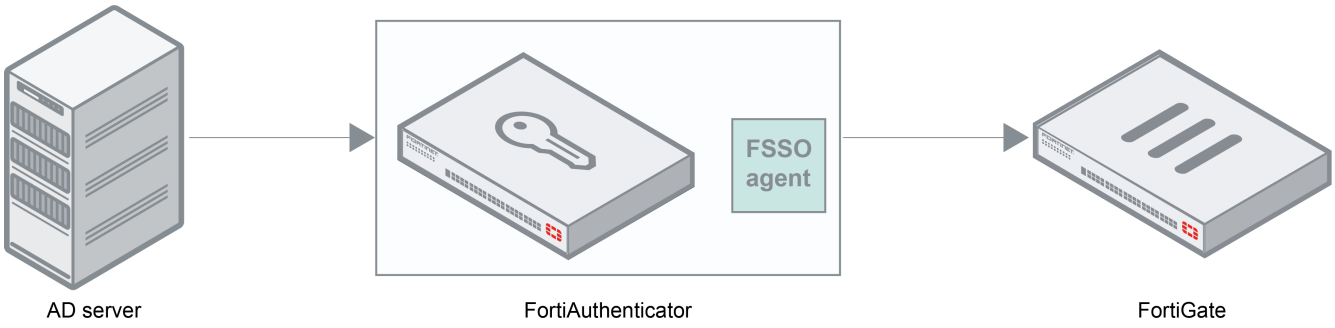
FortiOS with external FSSO polling

As opposed to built-in FSSO polling, FortiOS also supports FSSO with external tools, such as FortiAuthenticator and a Windows machine with FSSO installed. This section describes the following scenarios:

- FortiOS and FortiAuthenticator on page 9
- FortiOS and FSSO CA on page 10

FortiOS and FortiAuthenticator

In this scenario, FortiOS communicates to FortiAuthenticator, which has the FSSO CA installed, which in turn communicates to an AD server. This is recommended for a large AD environment.



The advantage of this scenario is the FortiAuthenticator FSSO collects login events and monitors workstations for user logouts. This supports DC agent/TS agent, syslog sources, RADIUS accounting, multiple domain environments, SAML SSO, and FortiClient Mobility agent (also known as FSSOMA). Citrix is supported when utilizing TS agent. NTLM is supported, but only for one domain. NTLM is optionally used by FortiAuthenticator to authenticate FSSOMA clients.

For environments with a large amount of users where precise user control is required, use FortiClient SSOMA and FortiAuthenticator to monitor user login/off events.

FortiClient SSO Mobility agent

By using FortiClient Single-Signon (SSO) Mobility agent with FortiOS with FortiAuthenticator, polling accuracy is increased. This solution is sometimes called FSSO Mobility agent.

The FortiClient SSO Mobility agent is a feature of Fortinet Security Fabric and FortiClient Endpoint Security. The agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The FortiClient SSO Mobility agent communicates with FortiAuthenticator and not FortiOS. As a result, the *SSO Mobility Agent* option must be enabled in FortiAuthenticator.

FortiOS and FSSO CA

In this scenario, the AD server communicates with a Windows machine that has FSSO CA installed, which in turn communicates with a FortiGate. This scenario is recommended for a large AD environment.

The advantage of this scenario is the FSSO CA machine uses its own resources to collect login events and to monitor workstations for user logouts. This scenario supports TS, Citrix, RADIUS accounting, NTLM, and multiple domain environments. The disadvantage of this scenario is that in very large workstation environments or in environments with significant latencies, it may take too long to query workstations, which may delay logon collections and logoff detection.

For AD environments, it is recommended to preconfigure the filter on the CA server. This reduces the amount of data exchanged between the FortiGate and the CA server. It is not recommended to mix the filters configured on the CA site and on the FortiGate.

The CA server should have sufficient resources (memory and CPU) to accommodate user logins and workstation monitoring. The amount of resources necessary depends on the name, size, and number of monitoring groups for login events. It also depends on the workstations' response latency and network environment specifics for workstation monitoring.

To increase performance for an environment where bursts of login events are expected to be frequent (more than 1500 users at the same time), enable logon cache. The CA will query its own cache to find the user's group membership instead of querying the AD server.

Disable monitoring workstations with large numbers of active users. When workstation monitoring is enabled, the CA server queries each workstation to check if the user is still logged in. Depending on the number of workstations and their latency, the CA server may be delayed when obtaining user logoffs. Depending on the company policy, these delays may be long enough to render the detection useless, making it more efficient to disable monitoring workstations.

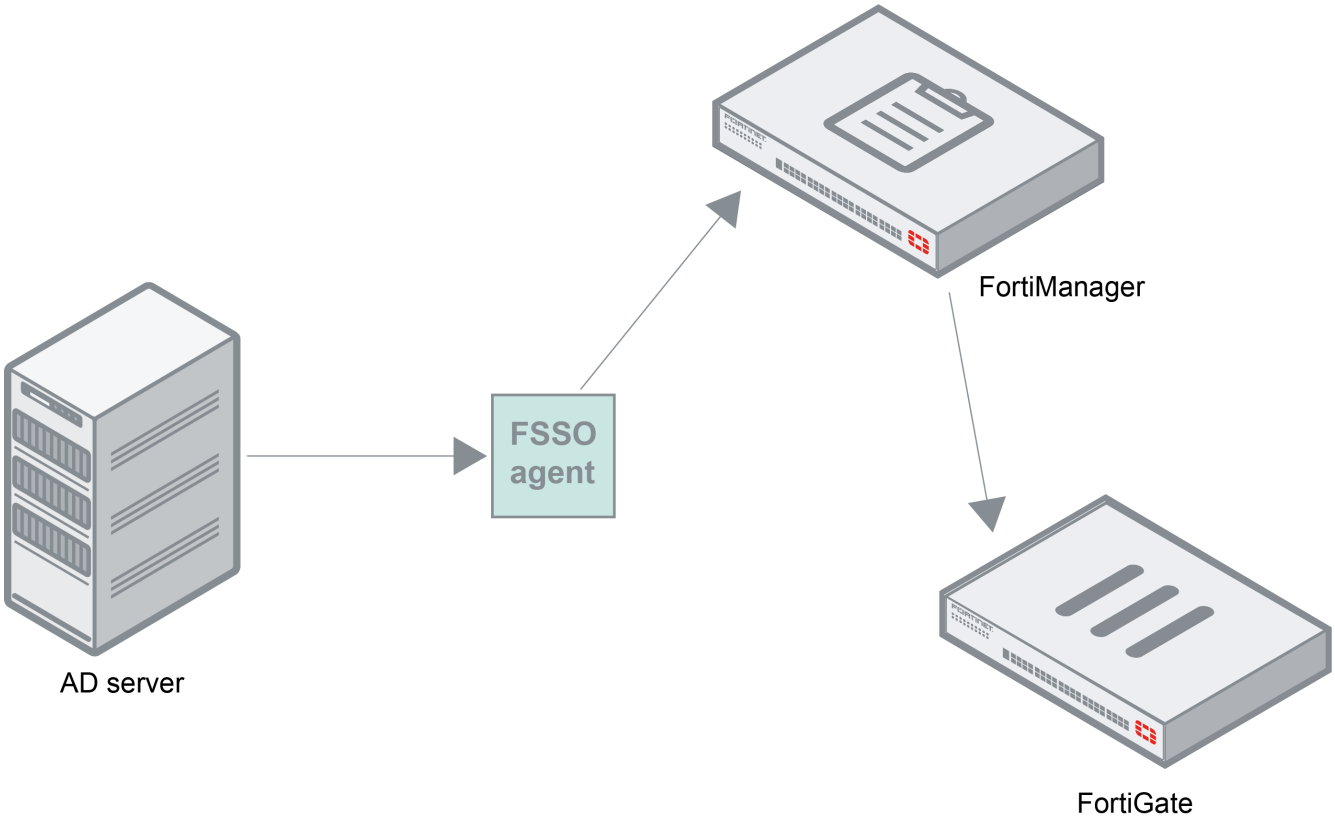
FortiManager, FortiOS, and FSSO

This section describes the different ways you can configure FortiManager to work with FortiOS and FSSO:

- FortiManager configured with access to FSSO CA on page 12
- FortiManager configured without access to FSSO CA on page 14

FortiManager configured with access to FSSO CA

This scenario is identical to FortiOS and FSSO CA on page 10, except that a FortiManager is also managing the FortiGates. In this scenario, FortiManager obtains information from the FSSO CA, then pushes it to the managed FortiGates. The AD server communicates to the FSSO CA. The AD server is accessible from FortiManager.



This mode is supported in FortiManager 5.4.0 and later versions.

This mode is recommended for environments where FortiManager is located physically near the CA server (and LDAP server if advanced mode is used) and latency is low. In this scenario, since FortiManager is close to the LDAP server, it

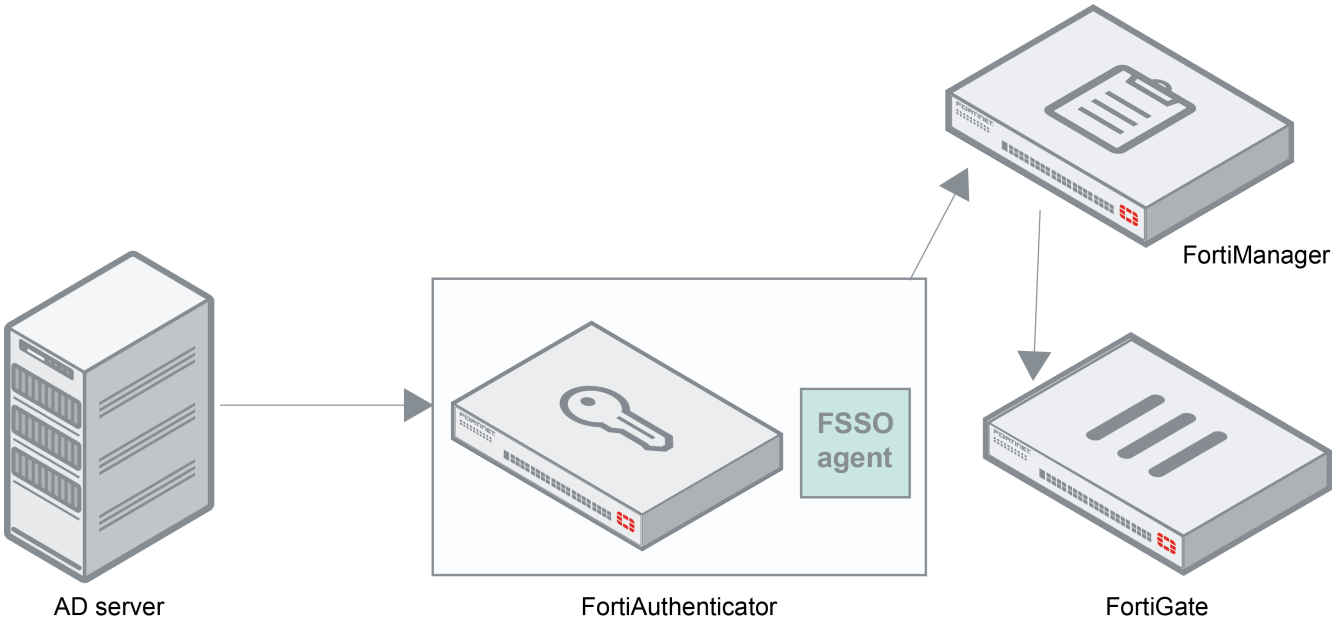
is better bandwidth- and performance-wise for FortiManager to poll the LDAP tree directly from the LDAP server if needed. Similarly, it is recommended that FortiManager poll groups directly from the CA server in standard mode or when LDAP is not accessible.

When using this setup, it is recommended to position the FortiGate physically close to the CA server (and LDAP server when advanced mode is used) so latency is low.

Ensure FortiManager can access the LDAP server when advanced mode is used. FortiManager needs access to the LDAP server to define FSSO groups. When FortiManager or FortiGate does not have access to the LDAP server, if using advanced mode, configure the FSSO group filter on the CA server, or use standard mode, which does not require LDAP access.

FortiAuthenticator support (CA server access)

This scenario is identical to FortiManager configured with access to FSSO CA on page 12, except that FortiAuthenticator provides additional security. In this scenario, FortiManager obtains information from FortiAuthenticator with FSSO CA, then pushes it to the managed FortiGates. The AD server communicates to the FortiAuthenticator with FSSO CA. The AD server is accessible from FortiManager.



This mode is recommended for environments where FortiManager is located physically near the CA server (and LDAP server if advanced mode is used) and latency is low.

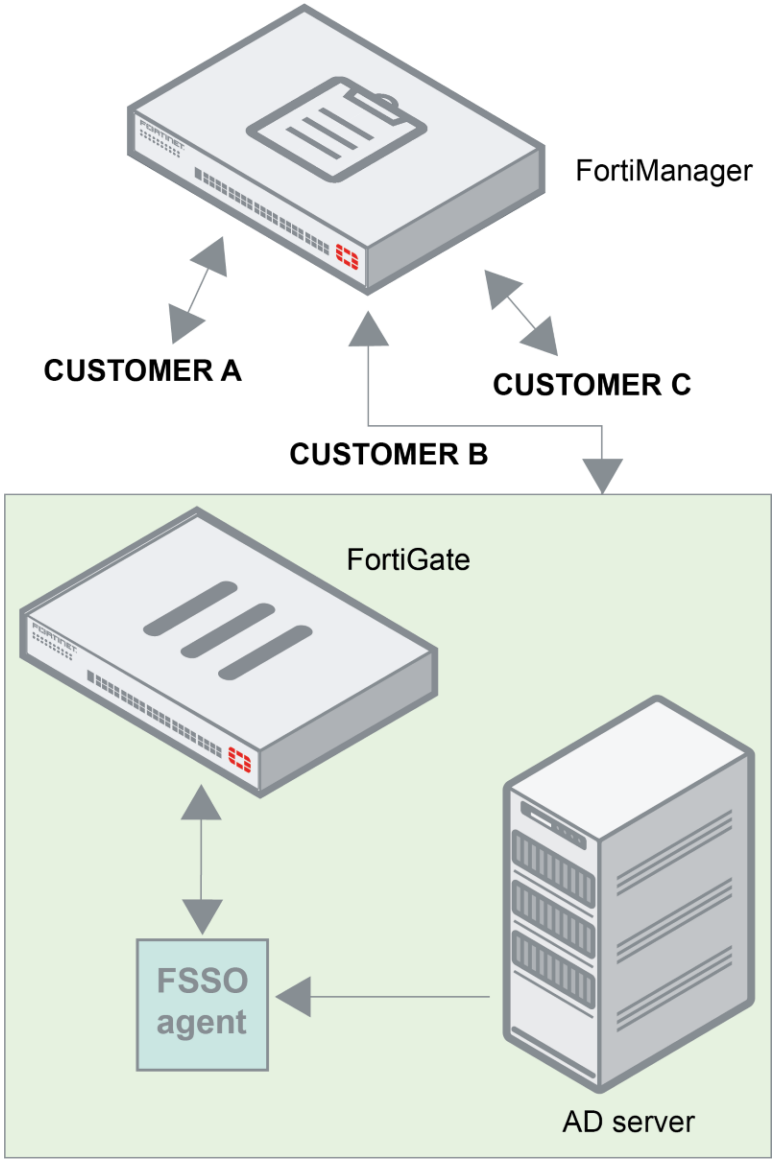
When using this setup, it is recommended to position the FortiGate physically close to the CA server (and LDAP server when advanced mode is used) so latency is low.

FortiAuthenticator manages the connection to the LDAP server to define the FSSO groups. The FSSO groups are then filtered to the FortiGate. When using FortiAuthenticator for FSSO, the FortiGate or FortiManager is never configured to directly connect to the LDAP server to define the FSSO groups.

When there is no access to the LDAP server, if using advanced mode, configure the FSSO group filter on the CA server, or use standard mode, which does not require LDAP access.

FortiManager configured without access to FSSO CA

This scenario is identical to FortiOS and FSSO CA on page 10 except that it also has FortiManager to manage the FortiGates. It is also similar to FortiManager configured with access to FSSO CA on page 12. However, here, FortiManager cannot directly access the CA server. This scenario is common in an MSSP environment where the FortiGate is located at the customer's site. The FortiGate has access to the AD server and FSSO CA, while FortiManager does not. FortiManager communicates to the FortiGate.



This mode is supported in FortiManager 5.4.3 and later versions.

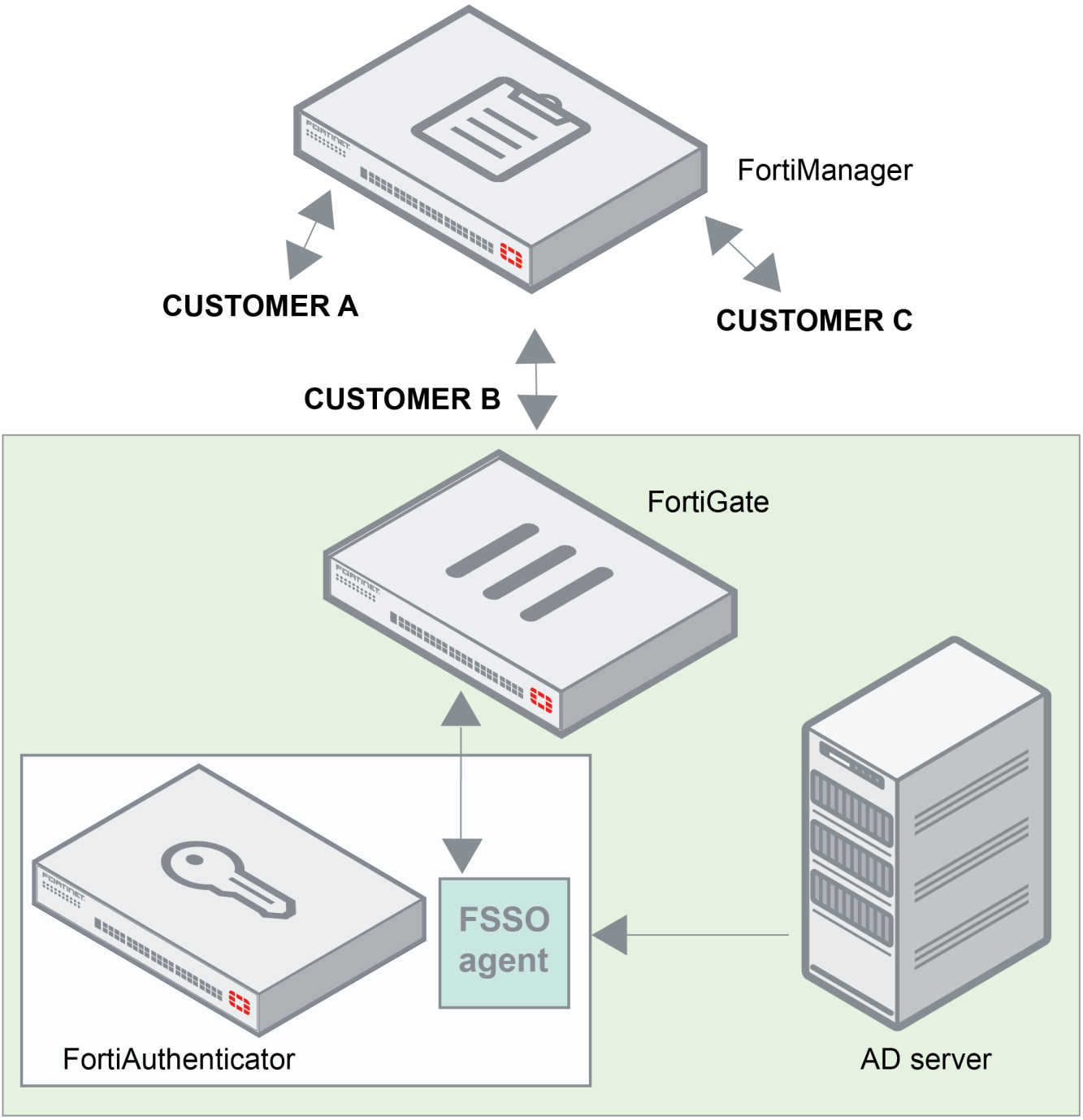
In this scenario, if FortiManager can still access the LDAP server, it can configure a filter for advanced mode and push it to the FSSO CA server through the FortiGate. For scenarios where FortiManager does not access the LDAP server and there is a bandwidth limitation or latencies, you may consider configuring the filter on the FSSO site. In both scenarios, FortiManager uses FortiGate to retrieve the filter information from the CA server.

When using this setup, it is recommended to position the FortiGate physically close to the CA server to keep latency low.

Ensure FortiManager can access the LDAP server when advanced mode is used. FortiManager needs access to the LDAP server to define FSSO groups. When FortiManager or FortiGate does not have access to the LDAP server, if using advanced mode, configure the FSSO group filter on the CA server, or use standard mode, which does not require LDAP access.

FortiAuthenticator support (CA server inaccessible)

This scenario is identical to FortiManager configured without access to FSSO CA on page 14 except that FortiAuthenticator is provides additional security. It is also similar to FortiAuthenticator support (CA server access) on page 13. However, here, the CA server is not directly accessible. This scenario is common in an MSSP environment where the FortiGate is located at the customer's site. The FortiGate has access to the AD server and FortiAuthenticator with FSSO CA, while FortiManager does not. FortiManager communicates to the FortiGate.



When using FortiAuthenticator for FSSO, all LDAP group connections are done through FortiAuthenticator and filtered to the FortiGate. FortiAuthenticator acts as the centralized authentication authority for users, two-factor authentication, FSSO users, and so on, which is all filtered back to the FortiGate. FortiManager then uses the FortiGate to retrieve the filter information from the CA server. When using this setup, it is recommended to position the FortiGate physically close to the CA server to keep latency low.